Loughborough University

This item was submitted to Loughborough's Research Repository by the author.
Items in Figshare are protected by copyright, with all rights reserved, unless otherwise indicated.

Privacy and data protection in e-commerce in developing nations: evaluation of different data protection approaches

PLEASE CITE THE PUBLISHED VERSION

http://www.infonomics-society.org/IJDS/

PUBLISHER

© Infonomics Society

VERSION

AM (Accepted Manuscript)

PUBLISHER STATEMENT

This work is made available according to the conditions of the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0) licence. Full details of this licence are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

LICENCE

CC BY-NC-ND 4.0

REPOSITORY RECORD

Adelola, Tiwalade, Ray Dawson, and Firat Batmaz. 2019. “Privacy and Data Protection in E-commerce in Developing Nations: Evaluation of Different Data Protection Approaches”. figshare. https://hdl.handle.net/2134/18623.

Privacy and Data Protection in E-commerce in Developing Nations: Evaluation of Different Data Protection Approaches

Tiwalade Adelola
Department of Computer Science
Loughborough University
Loughborough, UK
t.adelola@lboro.ac.uk

Ray Dawson
Department of Computer Science
Loughborough University
Loughborough, UK
r.jdawson@lboro.ac.uk

Firat Batmaz
Department of Computer Science
Loughborough University
Loughborough, UK
f.batmaz@lboro.ac.uk

Abstract

The emergence of e-commerce has brought about many benefits to a country's economy and individuals, but the openness of the Internet has given rise misuse of personal data. Several countries have enacted legislation and procedures to protect the information privacy of their citizens and corporations. However, many developing countries, such as Nigeria are yet to enact any procedures, despite the high level of identity theft and online fraud.
Different approaches to data privacy and protection are found in different countries. These can be generally categorised as the self-regulation approach, as used in the United States and the government approach, as used in the United Kingdom. This paper investigates the reasons why developed countries adopt any particular system for data protection. The paper evaluates these data protection approaches to determine its applicability in developing nations, using Nigeria as a case study. This is done by identifying the issues affecting data protection in the developing country and then evaluating the approaches' dispute resolution, enforcement and compliance monitoring processes for their applicability in the case of Nigeria. Benchmarks developed by the Australian government for Industry-Based Customer Dispute Resolution Schemes provide a suitable mechanism for evaluation.

Keywords-E-commerce; Data protection; Regulation; Nigeria;

1. Introduction

E commerce has many advantages of which the most important are the convenience and the global choice of goods and services and can exerted an increasingly important impact

on a country's economy. However, the emergence of e-commerce can also bring about a number of legal, socio-economic and trust issues, especially in developing nations where these issues pose significant challenges to the organisation of electronic commerce [1]. Many online businesses make use of customers' personal data to provide customised advertising, personalised services and strategic relationships with customers. According to the UK Data Protection Act [2], "Personal Data" is defined as "Data that relates to a living individual who can be identified from such data, or /and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual". Many customers are concerned about their personal data being used inappropriately, and this could reduce customers' trust in the website's services [3]. Fear about privacy and the lack of trust continue to be the biggest obstacles to the growth of online commerce. The Internet industry is built on trust between businesses [4]. These developments have forced several nations of the world to enact legislation and procedures to protect the information privacy of their citizens and corporations.

Due to the privacy trust issues, The Organisation for Economic Co-operation and Development (OECD), the U.S. government and the European Union began extensive discussions about developing a regulatory framework for privacy. These discussions were guided by eight privacy principles

i. Collection Limitation
ii. Data Quality
iii. Purpose Specification
iv. Use Limitation
v. Security Safeguards
vi. Openness
vii. Individual Participation
viii. Accountability

The European Union in 1995 decided to adopt formal enforcement in the form of the Data Protection Act [2] incorporating the eight OECD principles, while the United States, although endorsing the principles, adopted the self-regulation approach rather than governmental regulation [5].

The Nigerian Constitution recognises the right of privacy; however, Nigeria has neither enacted any specific data protection law nor adopted any functional self-regulatory system. There have been a number of drafted bills for e commerce personal data protection, but they

are yet to be effective [1]. The government and self-regulation approaches are evaluated in detail in this paper to determine why they may not be effective in developing nations.

2. Different data protection approaches

2.1. Self-Regulation approach

In the self-regulation approach, data protection in an e commerce context is left mostly to the evolution of industry norms and voluntary compliance. This approach is being used in the United States. Each company is responsible for deciding on the degree of information that is collected and used, and for developing its own privacy policy statement based on its industry guidelines [6]. There is no legal requirement in the U.S. for commercial websites or online service providers to maintain privacy policies. Due to the absence of data protection legislation, U.S. companies are adopting alternative means of assuring their customers of proper privacy practices. Third party organisations, for example TRUSTe and WebTrust, promote privacy practices and many U.S. websites display a Web seal to signal their compliance with the privacy standards formulated by the organisation [6].

2.2. Government Regulation approach

Many European countries have created strict privacy laws. Directive 95/46/EC of the European Council was issued on 24 October 1995. It deals with issues on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The UK Government was required to implement this Directive, which it did in the form of the Data Protection Act in 1998. It came into force on 1st March 2000. This totally replaced the previous Data Protection Act of 1984 [4].

The Information Commissioner, a British Government agency, enforces the privacy law. Any owner of a website based in the United Kingdom that collects personal information is required by law to inform the Information Commissioner and abide by the eight principles of the Data Protection Act [6]. The principles provide guidelines and specifications for collecting and processing personal data and all e-commerce websites are required to have a privacy policy that informs the website's visitors how data can be retained, processed, disclosed and removed in line with the principles.

3. Factors affecting a nation's data protection approach

Cultural values and privacy perceptions differ from country to country [3] [7]. These varying values exert a significant influence over how privacy is respected and treated in a given country. This, in turn, determines which data protection approaches a country adopts or if a

country has effective data protection. For example, the European Union's adoption of Europe-wide governmental regulation over protecting consumer data privacy may be interpreted as a reaction to the excesses of various oppressive regimes in the earlier part of the twentieth century, especially during World War Two, and the continuing fear of the misuse of personal data by corporate and government entities. The United States has leaned towards industry self-regulation, which could be rooted in the country's history of entrepreneurial behaviour and laizzez-faire capitalism [3]. Factors, such as the political changes in a country, can affect how privacy is viewed which influences the adopted privacy policy. Not all countries subscribe to the notion of privacy as a fundamental human right, which impacts the way a nation accepts the need to protect individual privacy rights. A nation's unique situation and issues of government, culture and even history should be considered for the implementation of a working data protection approach.

4. Issues Affecting Data protection in Nigeria

Nigeria has not yet enacted any specific data protection law. Some other African countries, such as Ghana, South Africa and Egypt, are ahead of Nigeria in data protection policies [8]. A draft guideline on a data protection bill was published by Nigeria's National Information Technology Development Agency (NITDA) in 2013 but it hasn't been passed into law and there is no establishment of an institutional framework [10]. A new cybercrime bill was introduced in 2013 with an update of provisions to the previous Computer Security and Critical Information Infrastructure Protection Bill of 2005. The draft legislation imposes certain security obligations on organisations operating computer systems and networks, but does not sufficiently address data protection [10].

As initially mentioned, a nation's socio-cultural and economic factors can determine a nation's regulatory approach. There are also reasons why a country may not view e-commerce data protection as a priority. Six suggested Nigerian factors that influence the inadequate data protection are discussed below. Five of these affect many, if not most, developing countries; the last is more particular to Nigeria.

4.1. Government Enforcement

Nigeria has not yet enacted any specific data protection law and neither is there any functional self-regulatory system [1]. The government has endorsed draft guidelines on data protection and cyber security in the past, but there is yet to be any legislation and there is no immediate prospect on it being passed as a law [1]. According to a survey carried out by Transparency International [11], 73% of the Nigerian population believes that the Nigeria legislative and parliamentary body is opaque and corrupt. This implies that even if legislation were enforced the population would not have confidence that it would be enforced effectively.

4.2. Political History

The political views of a country can affect its view on data protection [4]. The military of Nigeria has played a major role in the country's history, often seizing control of the country and ruling it for long periods of time. Data protection and fair information practice may not be widely accepted by totalitarian regimes. Although there was a political regime change in 1999 to democracy, the long-term totalitarian regime and the resulting ingrained attitudes could be a factor influencing the nation's slow adoption of a data protection policy.

4.3. Economic priorities

Nigeria, being a developing economy, is striving to provide the basic infrastructure of a steady supply of electricity, good roads and transportation, health, education services and postal and telecommunication networks, etc. [11] [12] that the enactment of a data protection policy would not be the government's highest priority.

4.4. Importance of personal Information and Information security

Some nations may or may not be overly concerned about the need for data protection to protect their citizens or corporations [14]. This is notable in the case of developing African nations, such as Nigeria, which lack privacy protection legislation. Studies have shown that regulatory responses usually occur in reaction to a growing level of information security concern within the masses [6] [12]. Milberg et al. also suggest that lower levels of information privacy concern will be associated with countries with no privacy regulation [6].
Nigeria is known for its high level of cybercrime, so many Nigerians are becoming aware of the dangers on putting credit/debit card details on just any website [9]. This has prompted many e-commerce websites to adopt the pay on delivery method [13]. This method provides peace of mind as no bank or card details are compromised. There should be concern about the absence of any protection or resolution in the case of the website misusing personal data.

4.5. Illiteracy and Lack of awareness

Nigeria is one the ten countries that contain the world's 775 million illiterate adults [14]. Many Nigerians are just beginning to understand what e-commerce is all about and thus they may not understand the concept of personal data protection in e commerce. Nigeria has also been identified as one of the fastest growing developing nations [15], so more and more people are starting to use the Internet, but the vast majority of the Nigerian population that use the Internet are unaware of the dangers associated with it [8]. Data protection systems should create awareness about the danger of data misuse and what proper data protection policy is.

4.6. Reputation and a Lack of Interpersonal Trust

The rapid development of the nation's IT infrastructure with the lack of regulation and enforcement has, unfortunately, led to Nigeria becoming a centre for cybercrime that has given the country a bad reputation for Internet users both within and outside Nigeria. This reputation and the lack of trust it generates creates a need for data protection, but at the same time, inhibits the population from trusting any scheme that could be put in place to protect personal data.

5. Australian Industry-Dispute Benchmarks

The benchmarks developed by the Australian government for Industry-Based Customer Dispute Resolution Schemes form a suitable foundation to evaluate consumer dispute regulation [20]. Cavoukian and Crompton [18] have used these benchmarks to evaluate the dispute resolution processes of three Web seals. These benchmarks cover the common content of international dispute resolution standards. The benchmarks are structured around six main principles:

Benchmark 1 — Accessibility: the scheme makes itself readily available to customers by promoting knowledge of its existence, being easy to use and having no cost barriers.

Benchmark 2 - Independence: the decision-making process and administration of the scheme are independent from scheme members.

Benchmark 3 - Fairness: the scheme produces decisions which are fair and seen to be fair by observing the principles of procedural fairness, by making decisions on the information before it and by having specific criteria upon which its decisions are based.

The key practices associated with Benchmark 3 specify that a dispute resolution scheme should be structured so that

1. The scheme's staff advises complainants of their right to access the legal system or other redress mechanisms at any stage if they are dissatisfied with any of the scheme's decisions or with the decision-maker's determination.
2. Both parties can put their case to the decision-maker.
3. Both parties are told the arguments, and sufficient information to know the case of the other party.
4. Both parties have the opportunity to rebut the arguments of, and information provided by, the other party.
5. Both parties are told of the reasons for any determination.
6. Complainants are advised of the reasons why a complaint is outside jurisdiction or is otherwise excluded.

Benchmark 4 — Accountability: the scheme publicly accounts for its operations by publishing its determinations and information about complaints and highlighting any systemic industry problems.

Benchmark 5 — Efficiency: the scheme operates efficiently by keeping track of complaints, ensuring complaints are dealt with by the appropriate process or forum and regularly reviewing its performance.

Benchmark 6 — Effectiveness: the scheme is effective by having appropriate and comprehensive terms of reference.

These benchmarks are used in the analysis of customer dispute resolution in sections 6 and 7 of this paper.

6. Evaluation of the United Kingdom's Government Approach

To enable adequate data protection mechanisms, there are some processes that any approach should perform: consumer dispute resolution, compliance monitoring and enforcement [15]. This paper examines these processes to determine what approach would be suitable for developing countries.

In nations where the data protection is regulated by the government, for example Austria, the Netherlands and the United Kingdom, the enforcement and compliance regulation is the responsibility of the government. As an example of a governmental, regulatory approach, the United Kingdom's Information Commissioner's Office (ICO) is examined in detail in the following:

6.1. Consumer Dispute Resolution

For a data protection approach to be effective there should be an appropriate method for customers to file complaints or concerns. It is also important that the complaints reach the appropriate personnel and are resolved promptly and suitably. If a customer discovers that their personal data managed by a Data Controller (online merchant) is inaccurate, or was processed illegally, the UK ICO's dispute resolution mechanism means the customer is entitled to [16]:

- Ask the Data Controller for the data to be corrected, erased or blocked.

- Demand that the Data Controller notify those who have already seen the incorrect data, unless this requires a disproportionate effort. A reasonable fee for providing access may sometimes be charged.
- If the customer does not receive an adequate answer from the Data Controller, they can submit a complaint to the ICO.

The authority must investigate complaints and may temporarily ban the data processing, which is the subject of the complaint. If the supervisory authority finds that data protection law has been violated, it can order the data be erased or destroyed and/or it can ban further processing.

An evaluation of the government regulatory system for use in Nigeria using the Australian Industry-Dispute Benchmarks gives the following:

Benchmark 1 — Accessibility: For a system to work in Nigeria it has to be easily accessed and it should create awareness about data misuse and how to forward complaints to the right authority. This could help create awareness on the importance of personal data protection and what rights a data subject has. Popular web seals like TRUSTe, require participants (data controllers) to display seals on their websites. The seal logo on the participating site links back to the seal's own website, which contains information about the available dispute resolution mechanisms. This system creates awareness about the dispute process.

Websites that conform to government regulations do not have an easily accessible system to provide customer dispute resolution, although some websites provide information to enable customers to file claims, ask questions and register complaints. This information is usually in the policy document, which in some cases isn't easy to find [6].

The lack of awareness of Personal Identifiable Information (PII) privacy issues in Nigeria means that few people would know how to register a complaint and the lack of importance given to information privacy issues means that any resolution of issues would be difficult to enforce.

Benchmark 2 — Independence: In self-regulating countries, if there is reason to believe that a site has not complied with its posted privacy commitments, the web seal owner, such as TRUSTe, may require an on-site compliance review by an independent third party, such as PriceWaterhouseCoopers [18]. In the UK, all of dispute resolution processes are handled solely by the Information Commission Office [18], although they occasionally work closely with other UK regulators where there is shared interest in regulatory action and data protection authorities in other countries [19].

With Nigeria dealing with economic issues such as corruption, electricity shortages, disputing data protection issues properly without external help may not be a priority [11]. A Nigerian equivalent of the ICO is unlikely to be given sufficient resources to fully resolve any issue.

Benchmark 3 — Fairness: The United Kingdom's Information Commissioner's Office seems to practice fair dispute resolution. According to the data protection Regulatory Action Policy document, it is indicated that they practice five principles of good regulation: transparency, accountability, proportionality, consistency and targeting [19]. The political history of Nigeria means that people will be reluctant to embrace transparency and the general lack of trust would mean that even if transparency was achieved it might not be trusted.

Benchmark 4 — Accountability: The Information Commissioner's Office posts dispute resolution decisions and complaint statistics, with brief summaries of the issues raised on its website. This includes detailed information on, monetary penalty, decision notices, trends, undertakings, enforcement notices and prosecutions given to various organisations [22]. They also have a news and event session with stories about high profile online privacy incidents. With Nigeria's political history, it is clear that there would be a reluctance to be so open, and even if this openness were achieved the lack of interest in privacy issues would mean it would be unlikely to achieve the same impact as in the UK.

This benchmark insinuates transparency. Nigeria is known for its government's lack of transparency [9] [10]. Even if the government is fully responsible for posting dispute resolution decisions and complaint statistics it is likely that customers will not fully trust it.

Benchmark 5 — Efficiency: The Information Commissioner's Office publishes a complaints performance document on its website. This shows the annual casework created and finished. They also show how long it takes for them to finish casework [23]. The pressures on a developing country's government are such that data privacy is unlikely to be given the priority to ensure an ICO equivalent could reach this level of efficiency.

Benchmark 6 — Effectiveness: The Information Commissioner's Office has detailed terms of reference. However, in Nigeria, the lack of appropriate legislation and the low priority to be given such legislation means that an equivalent of the UK's ICO could not be as effective.

Table 1 summarises the evaluation discussed.

Table 1.Evaluation of ICO's Dispute resolution Practices

Benchmarks	**ICO's Dispute Resolution practices**	**Nigeria's factor**
Accessibility	Not easily accessible dispute resolution scheme Usually located at a not easily accessible privacy policy	Lack of Personal Identifiable Information misuse awareness Lack of Personal Identifiable Information importance
Independence	Dispute resolution processes are handled solely by the ICO	Current economic issues may prevent proper sole dispute resolutions
Fairness	ICO practices fair dispute resolution practices	There may not be fair practices due to Government history and priorities
Accountability	ICO posts dispute resolution decisions complaint statistics, and brief summaries of the issues raised on its website	Government known for its lack of transparency
Efficiency	ICO publishes a complaints performance document on its website	Economic issues may prevent effectiveness in this regard
Effectiveness	ICO has detailed terms of reference	Lack of any legislation could hinder effectiveness

6.2. Compliance Monitoring and Enforcement

In order to ensure good privacy practices from organisations, rigorous compliance and enforcement functions must be in place [12]. Strong compliance and enforcement processes enhance the privacy principles and dispute resolution mechanisms by strengthening the consumer's trust. Compliance monitoring refers to those processes designed to ensure that the claims made by the data controllers on their websites are adequate, and that they are complying with the claims they have made to their customers relating to information protection, transaction integrity, business and information practices. Enforcement comes into play when the compliance process has gathered sufficient evidence that a website has been unable to adhere to the claims made to its customers [18].

Caukovian and Crompton [18] evaluated the self-regulation system elements of the compliance and enforcement functions for registration, standards, objectives, processes, and enforcement. However, for a government-regulated system, only registration, processes and enforcement are of interest. The standards and objective elements describe the aims and objectives and not the practical aspects of compliance monitoring and enforcement.

Registration: Web seal organisations, like TRUSTe, will initially review the website for adherence to TRUSTe programme principles and privacy statement requirements and also require the data controller to complete a self-assessment questionnaire [28]. In the UK, the Data Protection Act of 1998 requires every data controller who processes personal information to register with the Information Commissioner's Office [27]. The ICO provides guidelines and a checklist that data controllers can use to check how they are doing. The registration process, if the ICO's approach is adopted in Nigeria, could possibly work, but this, in itself, is not effective unless the ICO itself is an effective institution.

Processes: In the United Kingdom, the ICO conducts audits for public and private companies, public authorities and government departments. These audits are voluntary and are usually requested [26]. Although it is most suited to larger organisations with an understanding of the basics of compliance, the ICO also performs advisory visits for small to medium sized businesses. The visit is to give practical advice to organisations on how to improve data protection practice and also review what is carried out in practice [27]. Thirdly, the ICO encourages a self-assessment programme, which is aimed at promoting good personal data protection practice within sectors where there are a lot of smaller organisations or public authorities [28]. Most compulsory audits are initiated by public complaints.

In Nigeria, it is unlikely that there will be sufficient interest in privacy issues for website owners to regularly request an audit or a self-assessment programme. Compulsory audits may work in Nigeria, but only if the legislation was in place to make sure it happened. This is not likely to be a government priority in the immediate future.

Enforcement: The ICO investigates complaints and may temporarily ban any data processing, which is the subject of a complaint. If the ICO finds that data protection law has been violated, it can order the data be erased or destroyed and/or it can ban further processing. If the data controller refuses to make acceptable corrections or the breach is found serious, the ICO can issue a monetary penalty [17]. Clearly, there would be a lot of legislation necessary for such a scheme to be implemented in Nigeria, but this is unlikely in the near future. However, without this, the ICO cannot be effective.

Table 2 summarises the evaluation.

Table 2: Evaluation of ICO's Compliance Monitoring and Enforcement Practices

	ICO's Practices	**Nigeria's Factors**
Registration	Every website that processes personal information to register with the ICO	This system can only work with an effective ICO type institution

Processes	ICO conduct voluntary advisory visits and audits	Little interest in PII security means website owners are unlikely to request audits
Enforcement	ICO can temporary or permanently ban processing	The lack of any enacted legislation may prevent proper implementation

7. Evaluation Of TRUSTE'S Data Protection Approach

7.1. TRUSTe

This is an independent, non-profit privacy organization dedicated to building users' trust and confidence on the Internet. It has developed a third-party oversight seal programme designed to ease users' concerns about online privacy and accelerate the growth of e-commerce. TRUSTe was originally founded by the Electronic Frontier Foundation and the CommerceNet Consortium. Its privacy seal program was launched in July 1997 [29].

7.2. Consumer Dispute Resolution

For a data protection approach to be effective there should be an appropriate method for customers to file complaint or concerns. It is also important that the complaints reach the appropriate personnel and are resolved promptly and suitably. If a customer discovers that their personal data managed by a Data Controller (online merchant) is inaccurate, or was processed illegally, TRUSTe's dispute resolution mechanism means they are entitled to:

- Confirm that the Website in question is a TRUSTe client.
- Verify that the complaint is a privacy matter relating to a TRUSTe client Website.
- Contact the TRUSTe client Website first.

If the TRUSTe member does not resolve the complaint appropriately, TRUSTe will review to check the complaint's eligibility and mediate a solution [31]. Penalties that TRUSTe could impose on the violator are suspension and even termination of their programme and/or notifying government authorities like FTC (Federal Trade Commission) in case the violator still fails to comply [31].

Evaluating TRUSTe's approach for application in Nigeria using the Australian Industry-Dispute Benchmarks gives:

Benchmark 1 — Accessibility: For a system to work in Nigeria it has to be easily accessed and it should create awareness about data misuse and how to forward complaints to the right authority.

TRUSTe requires participants (data controllers) to display seals on their websites. The seal logo on the participating site links back to the seal's own website, which contains information about the available dispute resolution mechanisms [31]. This system creates awareness of the dispute process. Details of TRUSTe's complaints mechanisms are accessible from their official website and hence from their seal logo's link. This also verifies that the website is really a TRUSTe participant.
Adopting a data protection system with a similar accessible and transparent approach could help create awareness about data misuse and how to complain to the right authority. This could help create awareness on the importance of personal data protection and what rights a data subject has.

Benchmark 2 — Independence*:* If there is reason to believe that a site has not complied with its posted privacy commitments, TRUSTe may require an on-site compliance review by an independent third party, such as PriceWaterhouseCoopers [18].

With Nigeria dealing with economic issues such as corruption, electricity shortages, etc., disputing data protection issues properly without external help may not be a priority. Sourcing external help to help solve disputes rather than relying solely on the government may be a good data protection system to adopt

Benchmark 3 — Fairness: TRUSTe seems to practice fair dispute resolution. They provide for each party to receive information about the arguments of the other, advice complainants of other avenues if any are available, and to be told the reasons for TRUSTe's decision. This substantially meets the requirements of benchmark 3 [32].

The political history of Nigeria and the lack of trust in the government could mean that people will be reluctant to embrace transparency and the general lack of trust would mean that even if transparency was achieved it may not be trusted. This may not be the case if handled by a third party organization.

Benchmark 4 — Accountability: TRUSTe publishes a generic annual transparency report that shows how many complaints were raised and how many were resolved [32]. Due to the lack of trust in Government, adopting a trusted non-government organisation like TRUSTe could be better approach.

Benchmark 5 — Efficiency: TRUSTe publish a transparency report that shows details about the annual complaint performance. This shows the annual casework created and finished. They also show how long it takes for them to finish casework [29].

The pressures on a developing country government are such that data privacy is unlikely to be given the priority to ensure its efficiency. It may be a better option to delegate this aspect to a third party organization such as TRUSTe.

Benchmark 6 — Effectiveness: TRUSTe has detailed terms of reference [29]. However, in Nigeria, the lack of appropriate legislation and the low priority to be given such legislation means it may not be effective. Assigning data protection to a non-government organisation could mean an effective term of reference.

Table 3 summarises the evaluation.

Table 3.Evaluation of TRUSTe's Dispute Resolution Practices

Benchmarks	**TRUSTe's Dispute Resolution Practices**	**Nigerian Factor**
Accessibility	Easily accessible seal logo that redirects to dispute resolution information	Adopting similar approach could increase awareness and PII importance
Independence	May require an on-site compliance review by an independent third party	Relying less on the government may be a way of dealing with the economic priority factor
Fairness	TRUSTe seems to practice fair dispute resolution.	Due to lack of trust and opaque government, people mat trust TRUSTe's approach more than that of their government
Accountability	Annual transparency report shows how many complaints were raised and how many were resolved	Government known for its lack of transparency. Reports by a non-government body are more likely to be trusted
Efficiency	Transparency report that gives details of annual complaint performance	May be a better option to delegate transparency reports to a third party organisation
Effectiveness	TRUSTe has detailed terms of reference.	Assigning data protection to a non-government organisation could become an effective term of reference

7.3. Compliance Monitoring and Enforcement

TRUSTe and the ICO have similar elements as far as compliance monitoring and enforcement elements, registration, processes and enforcement. But unlike the ICO, the registration and compliance monitoring are involuntary

Registration: TRUSTe will initially review the website for adherence to TRUSTe programme principles and privacy statement requirements and also require the data controller to complete a self-assessment questionnaire. This system provides information about the participant's privacy practices which will determine if the seal will be issued or not [31]. With the absence of effective data protection legislation, implementing a similar approach may be successful

Processes: Unlike the United Kingdom ICO that conducts requested voluntary audits and advisory visits [26], TRUSTe representatives periodically review the website to ensure compliance with posted privacy practices and program requirements and to check for changes to the privacy statement [31].

TRUSTe regularly "seeds" websites, which is the process of tracking unique identifiers in a site's database. Unique user information is submitted and results monitored to ensure that the website is practising information collection and uses practices that are consistent with its stated policies [30].

TRUSTe also relies on online users to report violations of posted privacy policies, misuse of the TRUSTe seal, or specific privacy concerns pertaining to a website [31] [30].
Duet to lack of a legislation to conduct and monitor compulsory audits, implementing the self-regulatory approach with the help of web assurance organisations to perform compulsory audits could be another approach

Enforcement: Depending on the severity of the breach, the investigation could result in an on-site compliance review by a CPA (Certified Public Accountant) firm and/or withdrawal of the site's seal/license. After TRUSTe has exhausted all escalation efforts, extreme violations are referred to the appropriate law authority [30] [31].

This approach tries to resolve enforcement issues without involving the government unless in extreme situations. With the present unlikeliness of data protection legislation in Nigeria, a non-government such as TRUSTe body could be responsible for issuing appropriate penalties. Table 4 summarises the evaluation.

Table 4. Evaluation of TRUSTe's Compliance Monitoring and Enforcement Practices

	TRUSTe's Practices	**Nigerian Factor**
Registration	Reviews the website and also requires the data controller to complete a self-assessment questionnaire	This may be a good alternative in the absence of an ICO type organisation
Processes	Periodically reviews the Web site to ensure compliance	Compulsory audits may be a good alternative as there is little interest in PII security
Enforcement	Conducts onsite compliance review depending on severity	A non-governmental body responsible for issuing appropriate penalties could be a viable alternative in the absence of any legislation

8. Conclusion

The Information Commissioner's Office (ICO) just provides guidelines and voluntary audits to ensure compliance. A compulsory audit usually takes place if a complaint is filed or if a public organisation is involved. When a customer has no idea of their rights as a data subject or the responsibility of a data controller, they may not file any complaints and the data controller's practices may go unchecked. Even if they do file a complaint, the legislation needs to be in place for an office equivalent to the UK's ICO to be able to effectively act against the website owner.

Although it is stated that all data controllers must register with the ICO, there was no mention on how to enforce this law. In Nigeria, it is possible that many data controllers would not see the need to register and, as long as there are no complaints, they would have no problem. In Nigeria's case, where there may be little awareness on personal information misuse and data protection rights, the voluntary system of the ICO may not be a suitable approach. The governmental regulatory approach through an institution equivalent to the UK's ICO is unlikely to be effective in a country such as Nigeria where government priorities will mean that such an office would be unlikely to be given the resources and legislation it needs to be effective, and where the country's economic situation and traditions mean that most people are either unaware of data privacy issues or are not sufficiently interested to take action.

TRUSTe's alternative approach ensures that the data controllers are adhering to their requirements by constant compulsory audits and self-assessment questionnaires, unlike the United Kingdom's ICO that just provides guidelines and voluntary audits to ensure compliance. In a case where the customer is oblivious to their rights, TRUSTe can still monitor the data controller's compliance and ensure good privacy practices.

As registering with a web assurance organisation, such as TRUSTe, isn't compulsory in practicing countries, many data controllers in Nigeria would not register and customers may then not have any means of complaint. In Nigeria's case where there may be little awareness on personal information misuse and data protection rights, the voluntary registration process of self-regulation may not be a suitable approach.

Any approach that may work in Nigeria should have a dispute resolution system that is very easy to access and understand and will involve less government involvement and a strict compliance monitoring system. This paper has shown that the self-regulatory approach is likely to be effective in Nigeria. Although some of the aspects of this approach such as the voluntary registration may seem ineffective. However, if voluntary registration became widespread and customers became more aware of the meaning of Web seals, then public and commercial pressure would encourage organisations to take up voluntary self-regulatory approach.

9. References

[1] T. Akomolade, "Contemporary legal issues in electronic commerce in Nigeria," IJEC, 2008.

[2] Legislation.gov.uk, "Data Protection Act 1998," 2012. [Online]. Available: http://www.legislation.gov.uk/ukpga/1998/29/section/1. [Accessed 29th January 2014].

[3] R. Sarathy and C. Robertson, "Strategic and Ethical Considerations in Managing Digital Privacy," *Journal of Business Ethics,* no. 46, p. 111–126, 2003.

[4] G. Steinke, "Data privacy approaches from US and EU perspectives," *Telematics and Informatics,* no. 19, pp. 193-200, 2002.

[5] V. Mayer-Schonberger and F. Cate, "Notice and consent in a world of Big Data," *International Data Privacy Law,* vol. 3, no. 2, pp. 67-73, 2013.

[6] K. Jamal, M. Maier and S. Sunder, "Enforced Standards Versus Evolution by General Acceptance: A Comparative Study of E-Commerce Privacy Disclosure and Practice in the United States and the United Kingdom," *Journal of Accounting Research,* vol. 41, no. 1, pp. 73-96, March 2005.

[7] S. J. Milberg, S. J. Burke, H. J. Smith and E. A. Kallman, "Values, personal information privary and regulatory approaches," *Communications of the ACM,* vol. 38, no. 12, pp. 65-74, 1995.

[8] (NITDA), National Information Technology Development Agency, "Guidelines on Data Protection Draft," National Information Technology Development Agency (NITDA), 2013.

[9] Wolf Park; Digital Jewels, "The 2014 Nigerian Cyber Threat Barometer Report,"2014.[Online].Available:http://www.wolfpackrisk.com/portfolio/2014-nigerian-cyber-threat-barometer-report/. [Accessed 25 June 2014].

[10] Transparency International, "Nigeria," 2013. [Online]. Available: http://www.transparency.org/gcb2013/country/?country=nigeria. [Accessed 30 June 2014].

[11] K. Uma and F. Eboh, "Corruption, economic development and emerging markets: evidence from Nigeria," *Asian Journal of Maanagement Sciences and Education,* vol. 2, no. 3, July 2013.

[12] V. Rudraswamy and D. Vance, "Transborder data flows: adoption and diffusion of protective legislation in the global electronic commerce environment," *Logistics Information Management,* vol. 14, pp. 127-136, 2001.

[13] C. Chiejina and E. Soremekun, "Investigating the Significance of the 'Pay on Delivery' Option in the Emerging Prosperity of the Nigerian e-commerce sector," *Journal of Marketing and Management,* vol. 5, no. 1, pp. 120-135, 2014.

[14] Central Intelligence Agency, "The world Factbook," 2012. [Online]. Available:https://www.cia.gov/library/publications/the-world-factbook/fields/2103.html#xx. [Accessed 30 April 2014].

[15] D. Hinshaw and P. Mcgroarty, "Nigeria's Economy Surpasses South Africa's in Size," 6 April 2014. [Online]. Available: http://online.wsj.com/news/articles/. [Accessed 30 June 2014].

[16] BBBOnline, "Mission & Vision," [Online]. Available: http://www.bbb.org/council/about/vision-mission-and-values/. [Accessed 18 May 2014].

[17] European commision, "Misuse of your personal data - redress," 2013. [Online]. Available: http://ec.europa.eu/justice/data-protection/individuals/misuse-personal-data/index_en.htm. [Accessed 07 May 2014].

[18] A. Cavoukian and M. Crompton, "Web Seals:A Review of Online Privacy programs," in *22nd International Conference on Privacy and Personal Data Protection*, Venice, 2000.

[19] Information Commisioner's Office, "Data Protection Regulatory Action Policy," Information Commisioner's Office, 2013.

[20] Australian Information Commissioner, "Guidelines for recognising external dispute resolution schemes under s 35A of the Privacy Act 1988," Office of the Australian Information Commissioner, Sydney, 2001.

[21] Ministry for Customs and Consumer Affairs, "Benchmarks for industry- based customer dispute resolution schemes," Ministry for Customs and Consumer Affairs, Canberra City, 1997.

[22] Infomation Commisioner's Office, "Enforcement," [Online]. Available: http://ico.org.uk/enforcement. [Accessed 20 June 2014].

[23] Information Commissioner officer, "Complaints performance," 2013. [Online].Available:http://ico.org.uk/about_us/performance/complaint_casework_performance. [Accessed June 2014].

[24] Information Commission Office, "Register (notify) under the Data Protection Act," [Online]. Available: http://ico.org.uk/for_organisations/data_protection/registration. [Accessed 20 June 2014].

[25] Information Commissoner's office, "What is an audit and how can I request one?," [Online]. Available: http://ico.org.uk/for_organisations/data_protection/working_with_the_ico/audits. [Accessed 7 May 2014].

[26] Information Commisioner's office, "Advisory visits," [Online]. Available:http://ico.org.uk/for_organisations/data_protection/working_with_the_ico/advisory_visits. [Accessed 7 May 2014].

[27] Information Commissioner's Office, "Self assessments," [Online]. Available:http://ico.org.uk/for_organisations/data_protection/working_with_the_ico/self_assessments. [Accessed 7 May 2014].

[28] B. Markert, "Comparison of Three Online Privacy Seal Programs," SANS Institute, 2002.

[29] TRUSTe. TRUSTe. [Online]. http://www.truste.com/about-TRUSTe/

[30] Lee Burgunder, *The Legal Aspects of Managing Technology.* Boulevard Manson: South Western Cengage Learning, 2010.

[31] TRUSTe. TRUSTe Program Requirements. [Online]. http://www.truste.com/privacy-program-requirements/program-requirements

[32] TRUSTe, "Truste Transparency Report: 2013," San Francisco, 2014